UNITED STATES DISTRICT COURT
for the
Middle District of North Carolina

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Andrea Elizabeth Kinsey DOB: 06/02/1992	)))) Case No. 20MJ 2 to)))

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment B.

located in the _____ Middle _____ District of _____ North Carolina _____ , there is now concealed *(identify the person or describe the property to be seized):*

See Attachment D.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☑ evidence of a crime;

☑ contraband, fruits of crime, or other items illegally possessed;

☑ property designed for use, intended for use, or used in committing a crime;

☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
	Possession of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Distribution of Child Pornography
18 U.S.C. § 2252A(a)(2)(A)	

The application is based on these facts:
Please see the attached affidavit.

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.
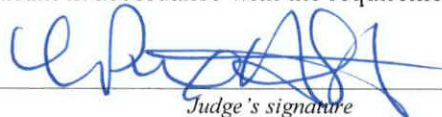
_____
/S/ Emily R. Keller
Applicant's signature

_____
Emily R. Keller, SPECIAL AGENT, FBI
Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 08/17/20 _____
Judge's signature

City and state: Greensboro, North Carolina _____ L. Patrick Auld, United States Magistrate Judge
Printed name and title

ATTACHMENT B

ANDREA ELIZABETH KINSEY

Andrea Elizabeth Kinsey, depicted above

DOB: 06/02/1992

ATTACHMENT D

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computers or storage media that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.

2. Routers, modems, and network equipment used to connect computers to the Internet.

3. Child pornography, as defined in 18 U.S.C. 2256(8).

4. Child erotica.

5. Records, information, and items relating to violations of the statutes described above in the form of:

   a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8), and/or child erotica;

   b. Records, information, and items referencing or revealing the occupancy or ownership of 323 Lockland Avenue, Winston-Salem, North Carolina 27103, including utility and telephone bills, mail envelopes, or addressed correspondence;

   c. Records and information referencing or revealing access to and/or use of BitTorrent;

   d. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;

e. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;

f. Records and information referencing or revealing communication or interaction of an illicit sexual nature with minors, to include the identity of the individuals involved and location of occurrence;

g. Records and information referencing or revealing participation in groups or the use of services that are known to be used to facilitate the trafficking of child pornography; and

h. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services.

6. For any computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

b. evidence of how and when the COMPUTER was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;

c. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

d. evidence of the Internet Protocol addresses used by the COMPUTER;

e. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

f. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

g. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

h. evidence of the lack of such malicious software;

i. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

7. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives,

flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Emily R. Keller, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

INTRODUCTION

1.   I am investigating offenses related to child sexual exploitation. This Affidavit is submitted in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises located at 323 Lockland Avenue, Winston-Salem, North Carolina 27103 (the "SUBJECT PREMISES"), more specifically described in Attachment A, the person of Andrea KINSEY (the "SUBJECT PERSON 1"), as more specifically described in Attachment B, and the person of David SPEASE (the "SUBJECT PERSON 2"), more specifically described in Attachment C, for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B), which items are more specifically described in Attachment D.

2.   The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of

securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located at the SUBJECT PREMISES, and/or on the SUBJECT PERSON 1, and/or on the SUBJECT PERSON 2.

AFFIANT BACKGROUND

3.   I am a Special Agent of the Federal Bureau of Investigation ("FBI"), and have been since October of 2019. My initial training consisted of an eighteen-week FBI new agent course during which I received instruction on various aspects of federal investigations, ranging from economic espionage and child pornography, to kidnapping and computer intrusions. In addition, I have earned both a Bachelor of Arts in International Studies and a Master of Public and International Affairs. I am currently assigned to the Charlotte Division and stationed at the Greensboro Resident Agency.

4.   As I am new to investigations involving child exploitation and child pornography, I am currently receiving training from FBI Special Agent Tara

S. Thomas, who has investigated child pornography cases for more than eight years.

5.   Prior to becoming a Special Agent of the FBI, I worked as a Staff Operations Specialist, investigative analyst, for the FBI for over four years. I have supported numerous FBI investigations through investigative research and analysis, to include investigations of cybercrime. I am familiar with, and have employed, investigative techniques used in these investigations, such as analysis of Internet Protocol addresses and Internet Service Provider records. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. § 2252A, and I am authorized by law to request a search warrant. As a Special Agent, I am authorized to investigate violations of laws and to execute warrants issued under the authority of the United States.

STATUTORY AUTHORITY

6.   As noted above, this investigation concerns alleged violations of the following:

a.   18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and

transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute.

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute.

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment D:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable

other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing

device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e.   "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f.   "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices

may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g.   "Computer-related documentation" consists of written, recorded, printed, or electronically stored material that explains or illustrates how to configure or use computer hardware, computer software, or other related items.

h.   "Computer software" is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

i.   A "Globally Unique Identifier" or GUID is a 128 bit number used by software programs to uniquely identify the location of a data object.

j.   "Geolocated," as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

k.   "Hashtag," as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

l.   A "Hash value" is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.

m.   The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet

often cross state and international borders, even when the devices communicating with each other are in the same state.

n. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

o. An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs

typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

p. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

q. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

r. "Peer-to-peer file-sharing" "P2P" is a method of communication available to Internet users through the use of special software. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. A user first obtains the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. A user obtains files by opening the P2P software on the user's computer, conducting searches for files that are currently being shared on another user's computer and then downloading files from the other user's computer.

s.   The terms "records," "documents," and "materials" include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies); mechanical form (including, but not limited to, phonograph records, printing, typing); or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, Bernoulli drives, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

t.   "Remote computing service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

u.   "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including

genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

v.   A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-ROMs, and other magnetic or optical media.

w.   "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

BACKGROUND ON PEER-TO-PEER FILING-SHARING AND BITTORRENT

8.   A known phenomenon on the Internet is peer-to-peer file-sharing ("P2P"). P2P file sharing is a method of communication available to Internet users through the use of special software programs. P2P file sharing programs allow groups of computers using the same file sharing network and protocols

to transfer digital files from one computer system to another while connected to a network, usually on the Internet. There are multiple types of P2P file sharing networks on the Internet. To connect to a particular P2P file sharing network, a user first obtains a P2P client software program for a particular P2P file sharing network, which can be downloaded from the Internet. A particular P2P file sharing network may have different P2P client software programs that access to that particular P2P file sharing network. Additionally, a particular P2P client software program may be able to access multiple P2P file sharing networks. These P2P client software programs share common protocols for network access and file sharing. The user interface, features, and configurations may vary between clients and versions of the same client.

9. In general, P2P client software allows the user to set up file(s) on a computer to be shared on a P2P file sharing network with other users running compatible P2P client software. A user can also obtain files by opening the P2P client software on the user's computer and conducting a search for files that are of interest and currently being shared on a P2P file sharing network.

10. Some P2P file sharing networks are designed to allow users to download files and frequently provide enhanced capabilities to reward the sharing of files by providing reduced wait periods, higher user ratings, or other benefits. In some instances, users are not allowed to download files that they

are not sharing. Typically, settings within these programs control sharing thresholds.

11. Typically, during a default installation of a P2P client software program, settings are established which configure the host computer to share files. Depending upon the P2P client software used, a user may have the ability to reconfigure some of those settings during the installation or after the installation has been completed.

12. Typically, a setting establishes the location of one or more directories or folders whose contents (digital files) are made available for distribution to other P2P clients. In some clients, individual files can also be shared. Typically, a setting controls whether or not files are made available for distribution to other P2P clients.

13. Typically, a setting controls whether or not users will be able to share portions of a file while they are in the process of downloading the entire file. This feature increases the efficiency of the network by putting more copies of file segments on the network for distribution.

14. Typically, files being shared by P2P clients are processed by the client software. As part of this processing, a hashed algorithm value is computed for each file and/or piece of a file being shared (dependent on the P2P file sharing network), which uniquely identifies it on the network. A file (or

piece of a file) processed by this hash algorithm operation results in the creation of an associated hash value often referred to as a digital signature. Some hash algorithms provide a certainty exceeding 99.99 percent that two or more files with the same hash value are identical copies of the same file regardless of their names. By using a hash algorithm to uniquely identify files on a P2P network, it improves the network efficiency. Because of this, typically, users may receive a selected file from numerous sources by accepting segments of the same file from multiple clients and then reassembling the complete file on the local computer. This is referred to as multiple source downloads. The client program succeeds in reassembling the file from different sources only if all the segments came from the exact copies of the same file. P2P file sharing networks use hash values to ensure exact copies of the same file are used during this process.

15.   P2P file sharing networks, including the BitTorrent network, are frequently used to trade digital files of child pornography. These files include both image and movie files.

16.   The BitTorrent network is a very popular and publicly available P2P network. Most computers that are part of this network are referred to as "peers." The terms "peers" and "clients" can be used interchangeably when

referring to the BitTorrent network. A peer can simultaneously provide files to some peers while downloading files from other peers.

17. The BitTorrent network can be accessed by computers running many different client programs, some of which include the BitTorrent client program, uTorrent client program and Vuze client program. These client programs are publicly available and free P2P client software programs that can be downloaded from the Internet. There are also BitTorrent client programs that are not free. These BitTorrent client programs share common protocols for network access and file sharing. The user interface, features, and configuration may vary between clients and versions of the same client.

18. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files. Depending upon the BitTorrent client used, a user may have the ability to reconfigure some of those settings during installation or after the installation has been completed. Typically, a setting establishes the location of one or more directories or folders whose contents (files) are made available to other BitTorrent network users to download.

19. In order to share a file or a set of files on the BitTorrent network, a "Torrent" file needs to be created by the user that initially wants to share the file or set of files. A "Torrent" is typically a small file that describes the file(s)

that are being shared, which may include information on how to locate the file(s) on the BitTorrent network. A typical BitTorrent client will have the ability to create a "Torrent" file. It is important to note that the "Torrent" file does not contain the actual file(s) being shared, but information about the file(s) described in the "Torrent," such as the name(s) of the file(s) being referenced in the "Torrent" and the "info hash" of the "Torrent". The "info hash" is a SHA-1 hash value of the set of data describing the file(s) referenced in the Torrent, which include the SHA-1 hash value of each file piece, the file size, and the file name(s). The info hash of each Torrent uniquely identifies the Torrent file on the BitTorrent network.

20. The Torrent file may also contain information on how to locate file(s) referenced in the Torrent by identifying "Trackers." Trackers are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the Torrent file. A Tracker is only a pointer to peers/clients on the network who may be sharing part or all of the files referenced in the Torrent. It is important to note that the Trackers do not actually have the file(s) and are used to facilitate the finding of other peer/clients that have the entire file(s) or at least a portion of the file(s) available for sharing. It should also be noted that the use of Tracker(s) on the BitTorrent network are not always necessary

to locate peers/clients that have file(s) being shared from a particular Torrent file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

21. Once a Torrent is created, in order to share the file(s) referenced in the Torrent file, a user typically makes the Torrent available to other users, such as via websites on the Internet.

22. In order to locate Torrent files of interest, a typical user will use keyword searches within the BitTorrent network client itself or on the websites hosting Torrents. Once a Torrent file is located that meets the keyword search criteria, the user will download the Torrent file to their computer. Alternatively, a user can also search for and locate "magnet links", which is a link that enables the BitTorrent network client program itself to download the Torrent file to the computer. In either case, a Torrent file is downloaded to the user's computer. The BitTorrent network client will then process the Torrent file in order to find Trackers or utilize other means that will help facilitate finding other peer/clients on the network that have all or part of the file(s) referenced in the Torrent file. It is again important to note that the actual file(s) referenced in the Torrent are actually obtained directly from other peers/clients on the BitTorrent network and not the Trackers themselves. Typically, the Trackers on the network return information about remote

peers/clients that have recently reported they have the same file(s) available for sharing (based on the SHA-1 info hash comparison), or parts of the same file(s), referenced in the Torrent, to include the remote peers/clients Internet Protocol (IP) addresses.

23.   For example, a person interested in obtaining child pornography images on the BitTorrent network would open the BitTorrent client application on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the Torrent search are typically returned to the user's computer by displaying them on the Torrent hosting website. The hosting website will typically display information about the Torrent, which can include the name of the Torrent file, the name of the file(s) referenced in the Torrent file, the file(s), and the "info hash" SHA-1 value of the Torrent file. The user then selects a Torrent of interest to download to their computer. Typically, the BitTorrent client program will then process the Torrent file. The user selects from the results displayed, the file(s) they want to download that were referenced in the Torrent file.

24.   Utilizing trackers and other BitTorrent network protocols (such as Distributed Hash Tables, Peer Exchange and Local Peer Discovery), peers/clients are located that have reported they have the file(s) or parts of the file(s) referenced in the torrent file available for sharing. The file(s) is then

downloaded directly from the computer(s) sharing the file. Typically, once the BitTorrent network client has downloaded part of a file(s), it may immediately begin sharing the file with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives "pieces" with the exact SHA-1 piece hash described in the torrent file. During the download process, a typical BitTorrent client program displays the Internet Protocol address of the peers/clients that appear to be sharing part or all of the file(s) referenced in the Torrent file or other methods utilized by the BitTorrent network protocols. The downloaded file is then stored in the area previously designated by the user and/or client program. The downloaded file(s), including the Torrent file, will remain until moved or deleted.

25. Typically, as described above, one method for an investigator to search the BitTorrent network for users possessing and/or disseminating child pornography files is to type in search terms, based on training and experience, that would return a Torrent file indicative of child pornography. The investigator would then download the file(s) referenced within the Torrent file and determine if the file(s) indeed contained child pornography. If so, the investigator can document the info hash SHA-1 hash value of this torrent file, to be compared with future identical Torrent files observed on the BitTorrent

network. Although transparent to the typical user, when searches are conducted, additional results are received from the trackers on other peers who recently reported to the network as having file(s) in whole or in part, which may include the IP addresses of those peers/clients. This information can be documented by investigators and compared to those info hash SHA-1 hash values the investigator has obtained in the past and believes to be child pornography. This allows for the detection and investigation of computers involved in possessing, receiving, and/or distributing files of previously identified child pornography. Therefore, without even downloading the file, the investigator can compare the info hash SHA-1 hash value and determine with mathematical certainty that a file(s) seen on the network is an identical copy of a child pornography file(s) they have seen before.

26. The returned list of IP addresses can include computers that are likely to be within the investigator's jurisdiction. The ability to identify the approximate location of these IP addresses is provided by geographic mapping services, which are publicly available and also used for marketing and fraud detection. At this point in the investigative process, an association between a known Torrent file (based upon the info hash value comparison) and a computer having a specific IP address (likely to be located within a specific region) can be established.

27.   Once a client user is identified as recently having a file(s) believed to be child pornography, in whole or in part, the investigator can then query the client user directly to confirm the client user has that file(s), in whole or in part, and/or download that file directly from the client user exclusively, otherwise known as a single source download. Depending upon several factors, including configuration and available resources, it might not be possible to do either. The process of sharing files on BitTorrent network involves peers allowing other peers to copy a file(s) or portions of a file(s). This sharing process does not remove the file(s) from the computer sharing the file. This process places a copy of the file on the computer which downloaded it.

28.   If an investigator either received an affirmative response from a remote peer that they possess a digital file, or the investigator received a digital file, in whole or in part, that is believed to contain child pornography, from a remote peer at a specific IP address, the investigator can conclude that a computer, likely to be in this jurisdiction, is running a BitTorrent P2P client and is currently possessing, receiving, and/or distributing specific and known depictions of child pornography.

29.   Law enforcement has created BitTorrent network client programs that obtain information from Trackers about peers/clients recently reporting that they are involved in sharing digital files of known actual child

pornography (based on the info hash SHA-1 hash value), which then allows the downloading of a file from a single IP address (as opposed to obtaining the file from multiple peers/clients on the network). This procedure allows for the detection and investigation of those computers involved in sharing digital files of known actual child pornography on the BitTorrent network.

30. During the query and/or downloading process from a remote BitTorrent network client, certain information may be exchanged between the investigator's client and the remote client they are querying and/or downloading from, such as 1) the remote client's IP address; 2) a confirmation from the remote client that they have pieces of the file(s) being requested, in whole or in part, and that the pieces of the file(s) is being reported as shared from the remote client program; and 3) the remote client program and version. This information may remain on the remote client's computer system for long periods of time. The investigator has the ability to log this information. A search can later be conducted on a seized computer system(s) for this information, which may provide further evidence that the investigator's client communicated with the remote client.

PROBABLE CAUSE

31. On February 20, 2020, an FBI undercover agent, known as an "Online Covert Employee" (OCE), used a BitTorrent application to conduct undercover investigations into the sharing of child pornography. During this investigation, a computer sharing child pornography was located on the BitTorrent file sharing network.

32. On February 20, 2020 at approximately 2:28 a.m., a computer belonging to the OCE made a secure connection with the computer at IP address 2607:fb90:528c:e21:5474:1115:8825:f0a6. Beginning on February 20, 2020 at approximately 2:28 a.m. through February 20, 2020 at 12:00 p.m., the OCE's computer downloaded 45 pictures and 36 videos directly from the computer at IP address 2607:fb90:528c:e21:5474:1115:8825:f0a6. Not all of the files were able to load.

33. On August 3, 2020, I reviewed the photographs and videos that the OCE downloaded from the computer at IP address 2607:fb90:528c:e21:5474:1115:8825:f0a6. I determined that there were 37 photographs and 26 videos containing child pornography. The below is the description of some of the photographs and videos identified:

> i. A photograph entitled "(pthc lolifuck) 6yr boy, 9yr girl, 33 yr dad 01(2)(2)" is a JPEG image that depicts a room with white

walls and yellow curtains. A prepubescent female child about the age of 9 is lying on her back, on a bed with white sheets. A prepubescent male child about the age of 5 or 6 is kneeling over her. The male child has his right hand on the bed besides the female child and his left arm is being held by an adult male. The female child, male child, and adult are not wearing clothing. The adult is kneeling on the bed behind the male child. The adult appears to be hunching over and looking at the male child's penis. The male child's penis is penetrating the female child's vagina. I deem this photograph to be Bondage, Discipline, Sadism, and Masochism (BDSM).

ii. A photograph entitled "boys 3some rbv kdv pt prt pthc pjk kids boy little hairless 03(2)(2)(3)(2)(2)" is a JPEG image that depicts three prepubescent male children about the age of 7 or 8 that are outside. There is grass on the ground. There are trees and a pond or lake in the background. One male child is kneeling. His clothing is below his knees. This male child's penis is penetrating the mouth of another male child, who is wearing a white shirt. The third male child is wearing a white

shirt and is lying near the other children. He is looking at the camera. I deem this photograph to be BDSM.

iii. A photograph entitled "pictures from ranchi torpedo dloaded in 2009- pedo kdv kidzilla pthc toddlers 0yo 1yo 2yo 3yo 4yo 5yo 6yo 9yo tara babyj(2" is a JPEG image that depicts a female toddler about the age of 2 lying on her abdomen. The toddler is not wearing clothing. An adult male, wearing a watch with a dark colored band, is behind her. The adult is not wearing clothing. His, what appears to be, erect penis is penetrating the toddler's anus. The adult's right hand is on the toddler's back and his left hand is on the toddler's left side. The toddler and adult appear to be on a pink, green, and purple blanket. I deem this photograph to be BDSM.

iv. A video entitled "!!new!!hussyfan pthc kinderficker i ass fuck my step doughter jeniefer sofie ver in bath an cum(2)" is a Video Clip lasting approximately 1 minute and 36 seconds and depicts a beige bathtub filled with water and white tiles on the wall. There is a toy on the left ledge of the bathtub. A prepubescent female child about the age of 4 is standing in the bathtub. An adult male is kneeling in the bathtub behind the child. The

adult and child are not wearing clothing. The adult has his right arm around the child's upper body and his left hand is on her knees. He places his erect penis through the child's legs against the child's genitalia. He moves his penis back and forth between the child's legs and uses his left hand to rub his penis against the child's vagina. He uses his right arm to move the child forward and penetrates the child's anus with his penis. He removes his penis from the child's anus and rubs it against the child's abdomen. He then ejaculates on the child's abdomen. I deem this video to be BDSM.

v. A video entitled "porno infantil - nina de 6 anos follada (pthc)" is a Window Media Audio/Video file lasting approximately 1 minute and 7 seconds and depicts a room with a computer tower near the ground. A prepubescent female child about the age of 4 is wearing a purple and white dress. The child's hands are on an adult male's erect penis. The adult masturbates his penis with his left hand. At approximately 24 seconds, the female child and adult male are in different positions. The child is lying on her back and her dress is raised above her hips. The child is not wearing underwear. The child's legs are apart and resting

on the adult's legs. The adult's erect penis is near the child's genitalia. The adult lifts the child's leg and rubs his penis on the child's vagina. He then spreads her legs apart and penetrates the child's anus with his penis. The adult puts his hands on her hips and moves the child up and down. I deem this video to be BDSM.

vi. A video entitled "pthc-jho-lolifuck) 10 yo katrina - doggystyle (new 2007)(2)" is a Windows Media Audio/Video file lasting approximately 29 seconds and depicts a room with light colored walls. There is a wooden chair with a floral fabric pattern on it in the background. A prepubescent female child about the age of 9 or 10 is wearing a white shirt. The child is on her hands and knees. An adult male, wearing a white shirt, is standing behind the child. Music is playing in the background. The adult appears to be penetrating either the child's vagina or anus from behind. He is holding the child's hips with his hands and moving her in a violent manner back and forth. The child is in distress as she screams and her eyes widen. I deem this video to be BDSM.

34. A query of the American Registry for Internet Numbers ("ARIN") online database revealed IP address 2607:fb90:528c:e21:5474:1115:8825:f0a6 as being registered to T-Mobile USA, Inc.

35. On February 20, 2020, an administrative subpoena was served on T-Mobile USA, Inc. requesting subscriber information for IP address 2607:fb90:528c:e21:5474:1115:8825:f0a6 on the following dates and times: February 20, 2020 from 2:28 a.m. through February 20, 2020 at 12:00 p.m. As a result of the subpoena, T-Mobile USA, Inc. provided the following account information.

Subscriber Name: ANDREA KINSEY
Subscriber Address: 323 Lockland Avenue, Winston-Salem, North Carolina 27103
Telephone Number: (336) 995-8476

36. The T-Mobile USA, Inc. records indicate that IP address 2607:fb90:528c:e21:5474:1115:8825:f0a6 was assigned to the account of Andrea KINSEY.

37. On July 30, 2020, I observed the residence located at the SUBJECT PREMISES. The residence is a one-story single-family home with gray siding. The numbers "323" are prominently displayed on the post near the door. The property is listed in Forsyth County Tax Department as deed book 1929, page 883, parcel number 6825632320000.

38.   A check of publicly available databases show KINSEY, date of birth 06/02/1992, and David SPEASE, date of birth 12/20/1980, as living at the SUBJECT PREMISES. On July 30, 2020, I observed one vehicle at the SUBJECT PREMISES, which was registered to KINSEY and SPEASE.

39.   On July 30, 2020, the North Carolina Department of Motor Vehicles (NCDMV) was queried regarding SUBJECT PERSON 1 and 2. Both had driver's license registered at the SUBJECT PREMISES. On August 11, 2020, surveillance observed SUBJECT PERSON 2, identified as David SPEASE from his NCDMV picture, exit the residence via the front door to check the mailbox on the front porch and return inside. Later that day, SUBJECT PERSON 2 exited the residence again to receive a FedEx package and returned inside.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

40.   I have had both training and experience in the investigation of computer-related crimes, as well as that of other agents assisting in the investigation. Based on my training, experience, and knowledge, I know the following:

a.   Computers and digital technology are the primary way in which individuals interested in child pornography interact with each

other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and computers with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d.   The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e.   The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f.   Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud"

storage) from any computer or smartphone with access to the Internet. Such an account can also be accessed in the same way. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g.   A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as "apps." Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored

h.   As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic

communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

  i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the Internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

41.   As described above and in Attachment D, this application seeks permission to search for records that might be found at the SUBJECT PREMISES, and/or on the SUBJECT PERSON 1, and/or on the SUBJECT PERSON 2, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

42.   I submit that if a computer or storage medium is found at the SUBJECT PREMISES, and/or on the SUBJECT PERSON 1, and/or on the SUBJECT PERSON 2, there is probable cause to believe those records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a.   Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b.   Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c.   Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d.   Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

43.   As further described in Attachment D, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium at the SUBJECT PREMISES, and/or on the SUBJECT PERSON 1, and/or on the SUBJECT PERSON 2 because:

a.   Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices

or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the

computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's

state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer

behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e.   Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f.   I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

44. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process that requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software, or operating system that is being searched;

b.　　Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c.　　The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d.　　Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users

can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

45. Additionally, based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of wireless routers, which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be secured (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or unsecured (in that an individual may access the wireless network without a key or password), wireless routers for

both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.
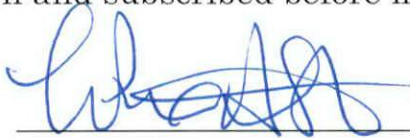
46.   Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

47.   Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment D, are located at the SUBJECT PREMISES, more fully described in Attachment A, and/or on the SUBJECT PERSON 1, more fully described in Attachment B, and/or on the SUBJECT PERSON 2, more fully described in Attachment C. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the SUBJECT PREMISES, the SUBJECT PERSON 1, the SUBJECT PERSON 2, and the seizure of the items listed in Attachment D.

/S/ Emily R. Keller
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me telephonically this ⎣7⎦ day of August 2020.

L. Patrick Auld
United States Magistrate Judge
Middle District of North Carolina